

**UNITED STATES DISTRICT COURT FOR THE
NORTHERN DISTRICT OF OKLAHOMA**

UNITED STATES OF AMERICA,)	
)	
Plaintiff,)	
)	
v.)	Case No. 19-CR-0103-CVE
)	
RAMAR TREVELLE PALMS,)	
)	
Defendant.)	

OPINION AND ORDER

Now before the Court is Defendant’s Motion to Suppress Evidence pursuant to a State Search Warrant and Brief in Support (Dkt. # 26). Defendant argues that evidence was seized from his cell phone based on a facially invalid warrant, and he asks the Court to exclude all evidence gathered during a search of his cell phone. Dkt. # 26. Plaintiff responds that the search warrant was sufficiently particular as to the place to be searched and the items to be seized and, even if the warrant is invalid, the good faith exception is applicable. Dkt. # 33. The Court set defendant’s motion for a limited evidentiary hearing “concerning the scope of the search of his cell phone that resulted from a search warrant obtained by the Tulsa Police Department (TPD).” Dkt. # 54. Plaintiff offered the testimony of two TPD officers and the Court finds that it has a sufficient evidentiary record to rule on defendant’s motion to suppress.

I.

On June 6, 2019, a grand jury returned an indictment (Dkt. # 2) charging defendant with sex trafficking by means of force, fraud, or coercion in violation of 18 U.S.C. § 1591 (count one), obstruction or attempted obstruction of enforcement of § 1591 (count two), and retaliation against

a witness, victim, or informant in violation of 18 U.S.C. § 1513 (count three). The charges stem from defendant's arrest on November 20, 2018 by an undercover TPD officer who was investigating potential human trafficking of young women in the commercial sex industry. TPD Officer Justin Oxford¹ set up a "date" with a prostitute who he believed could be a minor and a victim of human trafficking, and he agreed to meet the prostitute at the Peoria Inn in Tulsa, Oklahoma. Dkt. # 26-2, 2. When Oxford arrived at the Peoria Inn, he observed a black male sitting in a car in the parking lot, and he believed that the black male was conducting surveillance of Oxford as he approached the hotel room where he had agreed to meet the prostitute. Id. Oxford made contact with the prostitute, M.W., and arrested her after she agreed to perform a commercial sex act. Id. Oxford directed supporting officers to arrest the black male in the hotel parking lot, and the black male was subsequently identified as Ramar Palms. Dkt. # 33, at 2.

M.W. met Palms while she was a bartender at the Ambassador Lounge in Tulsa, and they began dating. Dkt. # 26-2, at 2. M.W. alleges that Palms took her to a hotel room and forced her to work as a prostitute. Id. M.W. told Oxford that Palms made her go on at least five "dates" every night and that he would provide security for her. Id. Palms allegedly assisted M.W. with posting advertisements for prostitution on websites, and he would make her pay to post the advertisements to distance himself from the prostitution. Id. M.W. told Oxford that Palms physically abused her if she did not generate enough business. Id. Palms kept note cards with contact information for customers of other prostitutes who had worked for him, and Palms would make M.W. call past customers on slow nights. Id.

¹ The facts stated in this section of the Opinion and Order come from the affidavit for search warrant prepared by Oxford unless otherwise noted.

Police officers seized Palms' phone when he was arrested and Oxford prepared an affidavit for search warrant (Dkt. # 26-2) to gather evidence of human trafficking from the cell phone. The affidavit states that the cell phone was in the possession of the TPD and the cell phone belonged to Palms. Dkt. # 26-2, at 1. Oxford sought the issuance of a search warrant to recover:

all digital evidence stored on removable storage and magnetic or electronic data contained in the contents of such tablet, cell phone, laptop, camera and/or memory cards, including electronic data storage devices, which in whole or in part contain any and all evidence related to the subscriber information from the SIM (subscriber identification module) and/or ownership information for the device, electronic mail, call logs, contacts, calendars, location services information, global positioning (GPS) data and information, internet chat communications, browser cache, auto-complete forms, stored passwords, instant messaging, SMS (short message service), MMS (multimedia message service), social media account data and information, application data and information, documents, photographs, images, graphics, pictures, videos, movies, audio or video recordings, any associated metadata, and any recorded documents depicting communications, correspondence or storage of these communications, files, graphics, documents, or other data related to the crime of **Human Trafficking**.

Id. The affidavit also seeks authorization to seize any evidence or data stored in "cloud" based accounts. Id. Oxford stated that recovery of data from a cell phone is complex and requires outside assistance, and he requested permission to take the cell phone outside of the jurisdiction for a forensic examination. Id. at 3. The warrant was issued by Tulsa County District Court Special Judge April Seibert on November 30, 2018. Dkt. # 26-1, at 2.

Defendant's cell phone was turned over to the special investigations division (SID) of TPD to obtain a forensic analysis of the cell phone. Officer Brian Booth is a member of SID who specializes in downloading data from seized cell phones, and he is certified to use various techniques for downloading data. Booth testified he initially takes a photograph of the evidence, takes the cell phone off any network, and checks the model number of the cell phone. Booth also reviews the

consent form or search warrant before attempting to extract any information or data from the cell phone. Booth plugs the cell phone into a machine to extract information from the cell phone, and he used a program called Cellebrite to perform the extraction. Cellebrite can perform three separate types of extraction, which he describes as logical, file, or physical extractions. He testified that logical and file extractions were more limited in nature, but these methods were not successful in this case and could not have obtained all information authorized by the warrant. Booth relied on the third type of extraction, known as physical, to retrieve data from defendant's cell phone, and this type of extraction pulled all information that could be obtained from the device, including content and metadata. Cellebrite prepared a report of the data gathered from the cell phone, and the data could be searched by file type (i.e. - text message, e-mail) and by using search terms. The warrant in this case also authorized the collection of cloud data, and this data was collected and stored as part of the search. The cloud data was contained in a separate report. Booth testified that he was not the investigating officer and he did not attempt to search any of the reports for relevant evidence. Instead, he used two other programs to conduct extractions to verify the accuracy of the data pulled from the phone, and he was also able to compare information on defendant's actual phone to verify the accuracy of the reports.

Oxford testified at the evidentiary hearing on the limited topic of his review of the reports containing the data extracted from defendant's cell phone. Oxford received multiple reports after data was extracted from the phone, and he reviewed the Cellebrite report of the physical data from the phone. Oxford did not look at the report containing the cloud data. Oxford explained that he could select what type of data from the report that he wished to search, such as text messages, photographs, or e-mails, and he could use search terms within those broader categories to expedite

his search. Oxford limited his search of the cell phone data to evidence of human trafficking, and did not encounter evidence of any unrelated crimes during his search. He did find personal communications of defendant during his search, but he immediately moved on when he found information outside the scope of the search warrant. Oxford learned from M.W. that her relationship with defendant began in September or October 2018, and he limited his search to communications that took place during the relevant time frame of September 2018 to November 20, 2018. Oxford prepared an officer's summary of what information he reviewed from the Cellebrite report, but he did not detail his methodology or specific dates of all communications that he reviewed in the report. Instead, it appears that his summary contains a list of potentially incriminating evidence against defendant that was found on his cell phone.² Oxford testified that he came across information that could be subject to attorney/client privilege during his review. Oxford immediately stopped searching and notified the Assistant United States Attorney (AUSA), Christopher Nassar, before resuming his search. Oxford reviewed short message service (SMS), multimedia message service (MMS), e-mails, and photographs from the relevant time period. Oxford has subsequently been reassigned to a new job, and he does not know if anyone else at TPD has reviewed the reports generated from defendant's cell phone.

II.

Defendant has filed a motion to suppress all evidence gathered from his cell phone, and he raises three general arguments in support of his motion. First, he argues that “document titled ‘Search Warrant’” is not actually a warrant and, even if the Court finds that it is a warrant, the

² Neither plaintiff nor defendant offered Oxford's summary as an exhibit at the evidentiary hearing.

document does not specify with sufficient particularity what evidence is to be seized. Dkt. # 26, at 4-8. Second, he argues that a forensic search of the entire contents of his cell phone exceeded the scope of the search authorized by the warrant. Id. at 9-10. Third, he argues that the good faith exception does not apply should the Court find that the warrant is facially invalid. Id. at 11-12. Plaintiff responds that the warrant complied with all of the requirements of the Fourth Amendment, and the good faith exception would apply if the Court found any technical error with the indictment. Dkt. # 33, at 4-9. Plaintiff also argues that the Tenth Circuit has issued guidance concerning the permissible scope of a forensic search of an electronic device, and it was reasonable for the forensic examiner to prepare a report concerning the complete contents of defendant's cell phone. Id. at 10-11.

A.

Defendant argues that the document that is styled as a "search warrant" fails to meet the basic requirements for a search warrant, because the document fails to specify the crime for which probable exists. Dkt. # 26, at 3. He further argues that the document fails to specifically identify the place to be searched, and it fails to include any language "commanding" or "authorizing" a search. Id. at 4. Plaintiff responds that there is no technical or special language required for a document to qualify as a search warrant as long the document meets the essential requirements provided by the Fourth Amendment. Dkt # 33, at 4-5.

The Supreme Court has determined that police must obtain a warrant before searching a suspect's cell phone. Riley v. California, 573 U.S. 373 (2014). In this case, Oxford sought a search warrant before submitting defendant's cell phone for a forensic examination, but defendant argues that the document signed by the state court judge was not actually a search warrant. The Tenth

Circuit has stated that the Fourth Amendment imposes four requirements that must be satisfied for the issuance of a valid warrant: “(1) the warrant must be based ‘upon probable cause,’; (2) the warrant must be ‘supported by Oath or affirmation,’ e.g., an affidavit; (3) the warrant must ‘particularly describ[e] the place to be searched,’; and (4) the warrant must ‘particularly describ[e] the . . . things to be seized.’” United States v. Cruz, 774 F.3d 1278, 1290 (10th Cir. 2014).³

Probable Cause

The search warrant (Dkt. # 26-1) states that “probable cause” had been found by the magistrate signing the warrant, but defendant argues that the warrant fails to specify for what crime probable cause was found. The Court has reviewed the search warrant and affidavit and finds that it is sufficiently clear that the magistrate found probable cause that defendant committed an offense involving human trafficking. Defendant is correct that the search warrant is somewhat vague as to the crime for which probable cause was found, as it identifies the crime as “Human Trafficking” as the offense and does not provide a statutory citation. The affidavit provides additional context for the crime allegedly committed by defendant, and it describes in detail the arrest of M.W. and the facts supporting Oxford’s belief that defendant had committed a human trafficking offense. Defendant attempts to read the search warrant in isolation, but the affidavit and search warrant provide sufficient notice of the alleged crime of which the magistrate found probable cause to believe defendant had committed.

³ It is not disputed that Oxford presented an affidavit to a magistrate, and the magistrate signed the affidavit to indicate that the affidavit was “[s]ubscribed and sworn to before” her on November 30, 2018. Dkt. # 26-2, at 3. The second Cruz element is not in dispute and need not be discussed in detail.

Because defendant has challenged the facial validity of the warrant, the Court will also consider whether the facts stated in the affidavit support a finding of probable cause. The Supreme Court has stated that probable cause is a “fluid concept-turning on the assessment of probabilities in particular factual contexts-not readily, or even usefully, reduced to a neat set of legal rules.” Illinois v. Gates, 462 U.S. 213 (1983). In the context of search warrants, the Tenth Circuit requires that a magistrate issuing a search warrant find that “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” United States v. Tisdale, 248 F.3d 964, 970 (10th Cir. 2001) (quoting Gates, 462 U.S. at 238). “Probable cause undoubtedly requires a nexus between suspected criminal activity and the place to be searched.” United States v. Corral-Corral, 899 F.2d 927, 937 (10th Cir. 1990). A magistrate may consider the affiant’s experience as part of her probable cause determination. United States v. Soussi, 29 F.3d 565, 569 (10th Cir. 1994). When reviewing the search warrant affidavit, this Court must “interpret [the affidavit] in a common sense and realistic fashion.” United States v. Grimmer, 439 F.3d 1263, 1270 (10th Cir. 2006). A reviewing court must show great deference to the magistrate’s finding of probable cause and the magistrate’s finding should be upheld if the magistrate had a “‘substantial basis’ for determining that probable cause existed.” United States v. Perrine, 518 F.3d 1196, 1201 (10th Cir. 2008) (quoting United States v. Artez, 389 F.3d 1106, 1111 (10th Cir. 2004)).

The affidavit states sufficient facts from which a neutral magistrate could have found probable cause to believe that defendant committed a human trafficking offense. Oxford stated that he set up a meeting with M.W. at the Peoria Inn, and he placed M.W. under arrest after she agreed to perform a commercial sex act. Dkt. # 26-2, at 2. He found defendant’s identification card in M.W.’s purse, and M.W. told Oxford that she met defendant when she was a bartender. Id. They

began dating and M.W. claims that defendant forced her to work as a prostitute. Id. Defendant allegedly directed M.W. to place advertisements on websites known for prostitution, and defendant had M.W. pay to place the advertisements to distance himself from the solicitation of prostitution. Id. M.W. alleged that defendant would physically abuse her if she did not go on enough “dates,” and defendant would threaten her if she did not go on at least five “dates” every night. Id. Defendant would have M.W. call former clients on slow nights in order to generate business. Id. A neutral magistrate could reasonably have concluded that probable cause existed to believe that defendant used means of force, fraud, or coercion to encourage M.W. to engage in commercial sex acts, and the Court finds that the warrant is supported by probable cause.

Place to be Searched and Items to be Seized

Defendant argues that the warrant authorized a general search of his phone, because the warrant fails to state with sufficient particularity the place to be searched and the items that could be seized. Dkt. # 26, at 5-7. The Fourth Amendment states that “[w]arrants shall . . . particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV. The Tenth Circuit has stated that “[o]ur test ‘for determining the adequacy of the description of the location to be searched is whether the description is sufficient to enable the executing officer to locate and identify the premises with reasonable effort, and whether there is any reasonable probability that another premises might be mistakenly searched.’” United States v. Garcia, 707 F.3d 1190, 1197 (10th Cir. 2013) (quoting United States v. Lora-Solano, 330 F.3d 1288, 1293 (10th Cir. 2003)). The particularity requirement is governed by the concept of “practical accuracy rather than technical precision,” and “[a] technically wrong address does not invalidate a warrant if it otherwise

describes the premises with sufficient particularity so that police can ascertain and identify the place to be searched.” United States v. Brakeman, 475 F.3d 1206, 1211 (10th Cir. 2007).

Courts have recognized that computer searches are “especially vulnerable to a worrisome exploratory rummaging by the government,” and the Tenth Circuit has drawn a “‘recognizable line’ in considering how much particularity is required for computer searches.” United States v. Russian, 848 F.3d 1239, 1245 (10th Cir. 2017). A search warrant for information on a computer must have some limiting principle, and a warrant seeking “‘any and all’ information, data, devices, programs and other materials” does not satisfy the particularity requirement. Id. However, a warrant may meet the particularity test if it limits the scope of the search to “evidence of specific federal crimes” or “specific types of materials.” Id. The Tenth Circuit has also recognized that it is not reasonable to require law enforcement officials to know where to search for potential evidence of a crime on a computer, and suspects may attempt to disguise or hide incriminating in innocuously named computer files to avoid detection during a search of the computer. United States v. Christie, 717 F.3d 1156 (10th Cir. 2013).

In a recent decision, the Tenth Circuit confronted the apparent dilemma between the particularity requirement of the Fourth Amendment and the difficulty with searching computers for relevant evidence. In United States v. Loera, 923 F.3d 907, 916 (10th Cir. 2019), the court acknowledged that limitations on the place to be searched work well in searches for physical objects, but computers store a vast amount of information and the information can be found almost anywhere on the computer. Id. at 916. Law enforcement agencies could reasonably seek a warrant to search the complete contents of a computer or electronic device, and traditional rules concerning the particularity requirement were not helpful in limiting the scope of searches of computers. Id. at 917.

Instead of applying rigid rules requiring particularity when seeking a warrant, the focus should be on the reasonableness of how the search is carried out by law enforcement officials. Id. An officer reviewing the contents of a computer may discover evidence of unrelated criminal conduct that is not within the scope of the warrant, but this does not require a court to find that evidence was illegally seized or that a warrant is invalid. Instead, a court should focus on whether law enforcement officials reasonably directed their search toward evidence specified in the warrant and did not become involved in a lengthy investigation that is not authorized by the warrant. Id. at 920. Police may be able to limit the scope of their search by starting a search in areas of a computer most likely to hold relevant evidence, and progressively expanding the scope of the search based on what they find in their initial search. Id. at 920.

The Court will consider defendant's arguments concerning the particularity requirement in reviewing the manner in which the search was carried out, because the warrant is not invalid under Loera merely because it permitted a search of essentially all areas of defendant's cell phone. Defendant argued at the evidentiary hearing that the warrant was so vague as to authorize a general search of his cell phone but, under Loera, this argument goes to the scope of the search rather than a facial defect with the warrant. The Court has considered defendant's arguments and does not find that the search warrant is facially invalid.

B.

Even if the Court were to find the warrant facially invalid, plaintiff argues that the officer who executed the search relied on the warrant in good faith and no evidence should be suppressed. There is a presumption that an officer relying on a warrant is acting in good faith and, although this presumption is not absolute, it "must carry some weight" with the Court. United States v.

McKneely, 6 F.3d 1447, 1454 (10th Cir. 1993). When an officer relies on a warrant issued by a neutral magistrate, the good faith rule should apply unless the “the underlying documents are ‘devoid of factual support’” or the officer’s reliance on the warrant was “wholly unwarranted.” Id. The good faith exception applies when “‘an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope,’ even though the search warrant was later deemed to be invalid.” United States v. Herrera, 444 F.3d 1238, 1249 (10th Cir. 2006) (quoting United States v. Leon, 468 U.S. 897, 920 (1984)). Excluding evidence obtained by police in good faith reliance on a search warrant would not deter future police misconduct and would penalize police for a magistrate’s error in issuing the warrant. Leon, 468 U.S. at 920-21. In Leon, the Supreme Court identified four exceptions to the good faith rule. If a warrant is invalid, the good faith rule does not prevent exclusion of evidence (1) “if the magistrate or judge issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;” (2) “where the magistrate wholly abandoned his judicial role in the manner condemned in *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979);” (3) in circumstances that “no reasonably well trained officer should rely on the warrant;” and (4) if a police officer relies on a warrant “so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.” Id. at 922-23.

The Court initially notes that it must distinguish between Booth’s and Oxford’s reliance on the warrant. Booth was the officer who extracted data from defendant’s cell phone, and he testified that he reviewed the warrant before attempting to download the contents of the phone. Booth testified that the warrant in this case was similar to warrants he has seen in other cases, and in many ways the warrant was more detailed than many warrants he reviews. Defendant argues that it should

have been apparent to Booth that the warrant was facially invalid, because the document contained no “command” language, failed to identify the crime for which probable cause was found, and was so broad that it should have been apparent that the warrant lacked sufficient particularity. Dkt. # 26, at 12. Defendant’s arguments are not compelling. Although the warrant does not “command” the search of a particular place, the document is styled as a search warrant and states that probable cause was found to believe that defendant committed the crime of human trafficking. “Human Trafficking” is found in bold type twice in the search warrant. Dkt. # 26-1, at 1. Warrants are generally interpreted for “practical accuracy rather than technical precision,” and the Court does not find that the lack of a “command” to search or the identification of the crime generically as “human trafficking” would alert a reasonable officer that it would be wholly unreasonable to rely on the warrant. See United States v. Ortega-Jimenez, 232 F.3d 1325, 1329 (10th Cir. 2000). The Court finds that Booth reasonably relied on the warrant as a basis to download the contents of defendant’s cell phone and, for the same reasons, finds that Oxford acted in good faith in reviewing the reports generated by Booth. The Court will separately consider defendant’s legal objections to the scope of the search authorized by the warrant but, based on the testimony of Booth, it does not appear that there was anything unusual about the scope of the search of defendant’s cell phone authorized by the warrant that would have alerted him that the warrant was facially invalid.

C.

Defendant argues that the search that resulted from the warrant obtained by Oxford was impermissibly broad, because the warrant authorized Booth to download the complete contents of defendant’s cell phone. Dkt. # 26, at 9. Defendant focuses on the techniques utilized by Booth to download the contents of the phone, rather than the subsequent search of the actual data performed

by Oxford. Plaintiff responds that it was reasonable for Booth to perform a physical download for essentially all of the data on defendant's cell phone, and Oxford appropriately limited his search of the report to evidence of the offense listed in the warrant. Dkt. # 33, at 10-12.

Under Loera, the Court reviews the particularity requirement of the Fourth Amendment by considering the language of the warrant and the scope of the search that actually resulted from the warrant. In this case, the search warrant sought the following information from defendant's cell phone:

all digital evidence stored on removable storage and magnetic or electronic data contained in the contents of such tablet, cell phone, laptop, camera and/or memory cards, including electronic data storage devices, which in whole or in part contain any and all evidence related to the subscriber information from the SIM (subscriber identification module) and/or ownership information for the device, electronic mail, call logs, contacts, calendars, location services information, global positioning (GPS) data and information, internet chat communications, browser cache, auto-complete forms, stored passwords, instant messaging, SMS (short message service), MMS (multimedia message service), social media account data and information, application data and information, documents, photographs, images, graphics, pictures, videos, movies, audio or video recordings, any associated metadata, and any recorded documents depicting communications, correspondence or storage of these communications, files, graphics, documents, or other data related to the crime of **Human Trafficking**.

Dkt. # 26-1, at 1. Defendant complains that the warrant authorized a general search of his phone without any restrictions as to which places in the phone could be searched. Dkt. # 26, at 10. However, Loera explains that traditional rules concerning the particularity requirement do not work well in the context of an electronic search, because a suspect can hide relevant evidence in an "infinite" number of places on a computer or electronic device and any file or program could contain relevant evidence. Loera, 923 F.3d at 916. The Court finds that defendant's objection to the scope of the warrant is misplaced to the extent that he relies on the particularity requirement of the Fourth

Amendment, because Oxford could reasonably have sought a warrant seeking access to the complete contents of defendant's cell phone. Booth testified that he was unable to use more limited search protocols, such as logical or file extractions, to download all of the data within the scope of the warrant. The Court does not find that the warrant is invalid for a lack of particularity, because the warrant authorized a search of all potential places on defendant's cell phone where relevant evidence could be found.

Defendant's argument is more appropriately considered in the context of the search that actually resulted from the warrant, and Booth and Oxford testified about this issue at the evidentiary hearing. Booth downloaded the contents of defendant's cell phone using Cellebrite, and he performed a physical extraction that downloaded all of the data on the phone. Booth did not attempt to review the data in an attempt to locate incriminating evidence, and his job was limited to downloading the data and verifying that the reports generated by Cellebrite accurately represented the contents of the cell phone. Booth used two other programs, Oxygen Forensics and Susteen Secure View, to extract data from defendant's phone, and he compared that data to the report generated by Cellebrite. Booth verified that Cellebrite had accurately recorded the data from defendant's cell phone, and he prepared a separate report for any cloud data. Defendant argues that Booth could have attempted more restrictive methods of downloading the data or he could have contacted another law enforcement agency to see if they had other more targeted means for searching the phone, but this argument misses the point. The search warrant authorized Booth to download the entire contents of the phone and, under Loera, this is permissible. Booth did not personally search the reports containing the actual data from the cell phone, and he performed a limited role as support staff with expertise in downloading data from electronic devices. The Court finds that Booth

did not exceed the scope of the warrant by conducting a complete download of the data on defendant's cell phone and the associated cloud data.

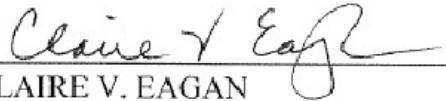
The key issue for both the issue of particularity and the scope of the search is the actual review of the Cellebrite reports by Oxford. Oxford received several reports concerning the data recovered from defendant's cell phone, but he did not look at the report describing the cloud data. He focused on the Cellebrite report containing data downloaded from defendant's cell phone, and he reviewed text messages, photographs, and e-mails recovered from the phone. Oxford limited his search to the time when M.W. claims that she had a relationship with defendant, and he avoided looking at messages or data outside of the time period of September 2018 to November 20, 2018. Oxford did not inadvertently discover evidence of other crimes during his search, and he did not conduct any side-investigations outside of his search for evidence related to human trafficking offenses. He did find personal communications from defendant to other persons, but he quickly moved on and did not conduct further investigation of unrelated personal matters of defendant. Oxford could expedite his search by using search terms, but it was necessary to view all of the communications from the relevant period as a whole to understand the context. Oxford prepared an officer's summary of potentially incriminating evidence on the cell phone, but the report does not otherwise explain his methodology for conducting a search of the cell phone data. Defense counsel questioned Oxford about whether he could have avoided reading e-mails that were not related to his investigation, but Oxford explained that the e-mails appeared in a preview window as he scrolled through the e-mails. Oxford came across materials that could be subject to attorney/client privilege. He immediately stopped searching the cell phone and contacted the AUSA before proceeding.

The Court finds that Oxford did not exceed the scope of the search warrant and his search was reasonable under the guidance provided by the Tenth Circuit in Loera. Oxford testified that he searched for evidence of human trafficking offenses, and his testimony establishes that he did not encounter evidence of other crimes or conduct investigations into unrelated matters. In Loera, the Tenth Circuit explained that in one previous case it had invalidated the search of an electronic device by a police officer, because the police officer found child pornography while searching for evidence of a drug offense. Loera, 923 F.3d at 917. The officer conducted a lengthy investigation into the child pornography and it should have been apparent after opening the first image that certain files would not contain relevant information within the scope of the warrant. Id. at 918. In fact, the officer began specifically searching for evidence related to the possession of child pornography and temporarily abandoned the search authorized by the warrant. Id. There is no evidence in this case suggesting that Oxford conducted an investigation into anything other than potential human trafficking offenses, and he limited his search to the relevant time period when the alleged offense occurred. Oxford testified that he searched text messages, photographs, and e-mails stored on defendant's cell phone, and these were likely locations where relevant evidence would be found. Oxford found some personal communications between defendant and other persons, but he moved on and did not investigate matters outside the scope of the search warrant. Oxford testified that he did discover attorney/client materials, and he immediately stopped his search and sought advice from the AUSA. At the evidentiary hearing, defense counsel focused on Booth's actions in downloading the entire contents of defendant's cell phone, and he made little or no argument concerning the scope of Oxford's search. Defendant has not shown that Oxford conducted a general search of defendant's

cell phone that exceeded the scope of the warrant, and his motion to suppress evidence seized as a result of the search of the cell phone should be denied.

IT IS THEREFORE ORDERED that Defendant's Motion to Suppress Evidence pursuant to a State Search Warrant and Brief in Support (Dkt. # 26) is **denied**.

DATED this 7th day of November, 2019.



CLAIRE V. EAGAN
UNITED STATES DISTRICT JUDGE